AUTOMOTIVE SECURITY ENGINEERING

Nice, 29th September 2009

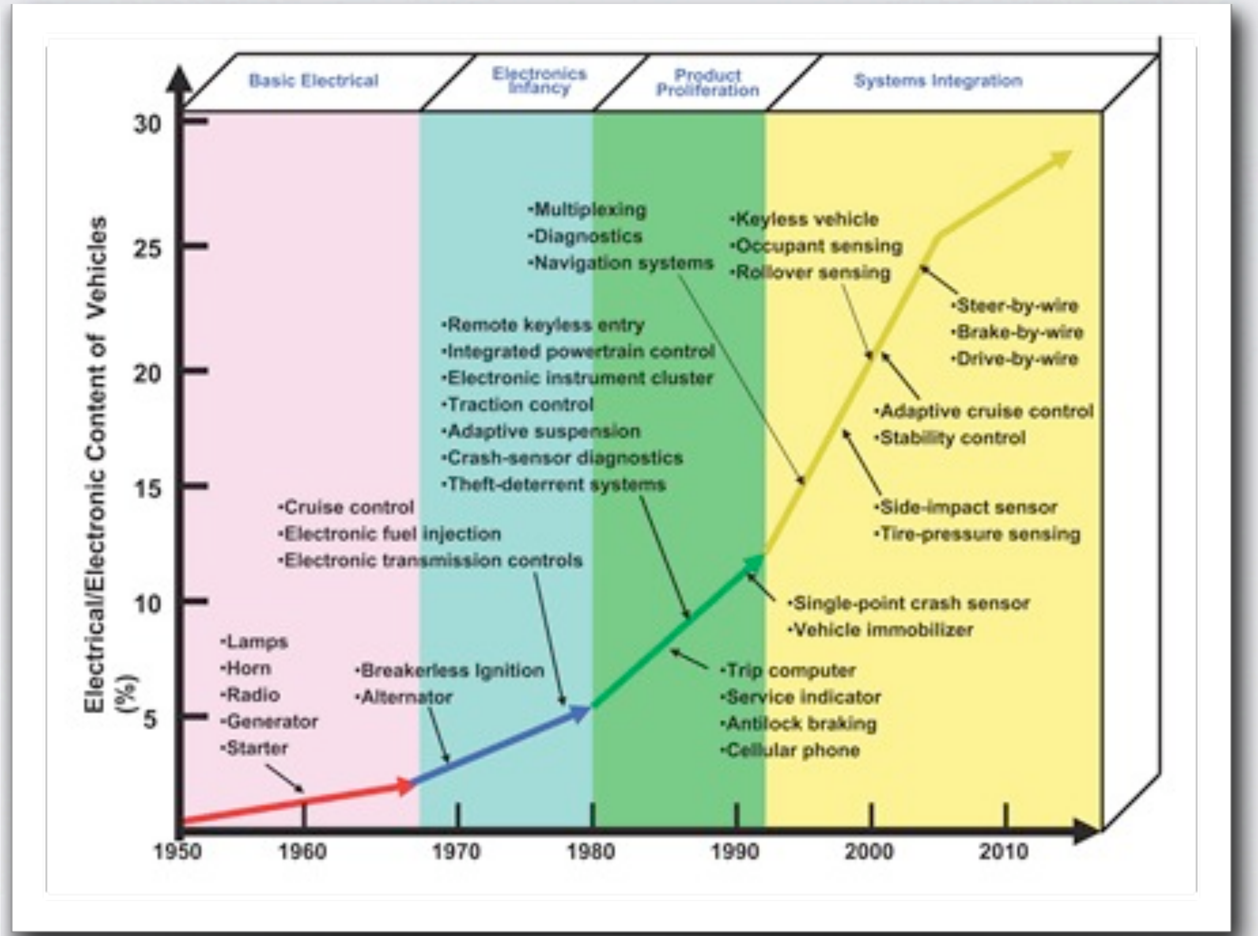
Martin Maas

PART I: INTRODUCTION

A short introduction into vehicular IT systems and automotive security

INTRODUCTION

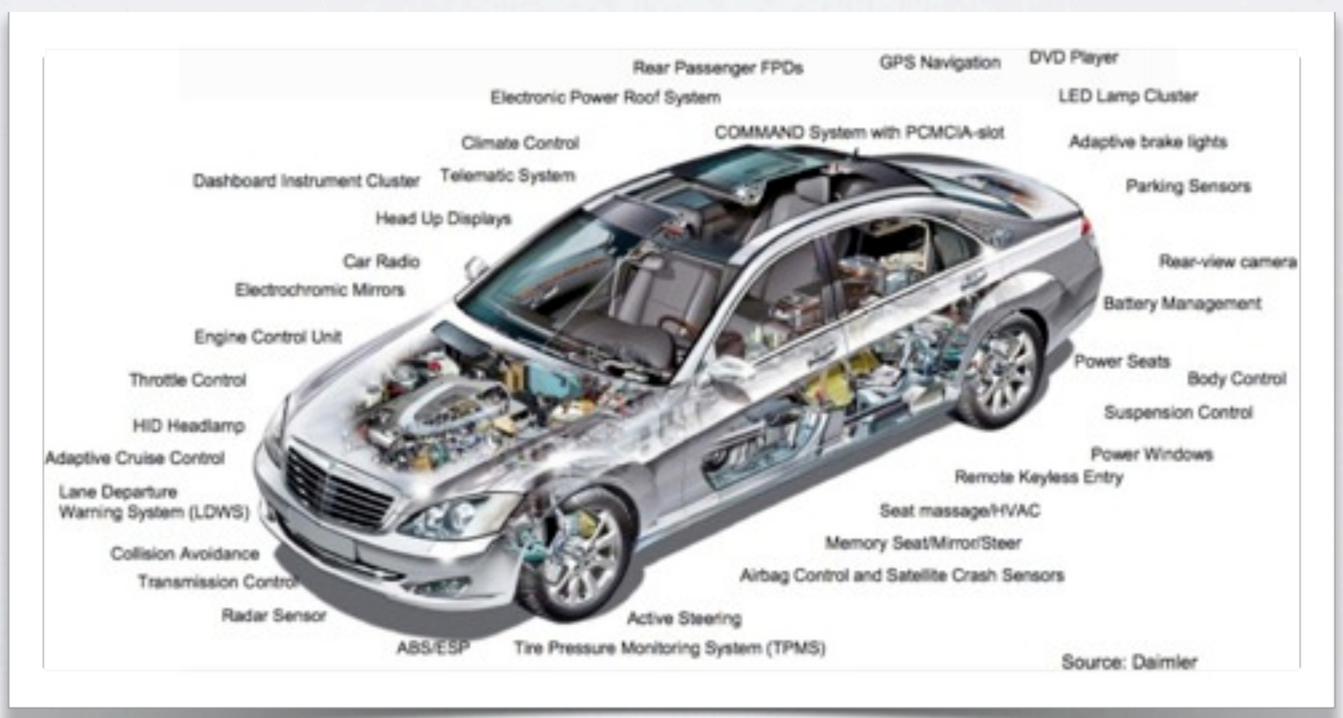
- Until the 70's cars were purely mechanical
- Today they are **mostly driven by software**



Source: ESL Development Gets A Leg Up, Chip Design Magazine, Dec/Jan 2005
http://chipdesignmag.com/display.php?articleId=57&issueId=8

INTRODUCTION

- Up to **80 processors**, **5 bus systems**, more than **100 MB of embedded code** performing more than **2000 individual functions**
- Systems usually incorporate **safety** features but exhibit lack of **security** ➔ Emerging field: **Security in Vehicular IT Systems**



The car of today and tomorrow, In-Vehicle LAN

OUTLINE

Part I: Introduction
A short introduction into vehicular IT systems and automotive security

Part II: Use Cases
Applications of vehicular electronics and automotive security

Part III: Security Engineering
Approaches to implement security mechanisms and peculiarities of automotive security

Part IV: Perspectives
The future of automotive security

Part V: Discussion
Questions and Free Discussion

DEFINITIONS

Security engineering is a specialized field of engineering that deals with the development of detailed engineering plans and designs for security features, controls and systems.

(Wikipedia)

- **Vehicular IT systems:**
  - **computer systems** within vehicles (e.g. cars, lorries, etc.)
  - perform a particular **functionality** inside that vehicle
  - are usually **embedded**

DEFINITIONS

IT Safety: protection against technical failures
(e.g. redundancy, fall-back mechanisms, self-testing, error detection,...)

↔

IT Security: protection against malicious encroachment
(e.g. authentication mechanisms, protecting integrity of data,...)

They are interleaved: Safety measures can enhance security, but can also be a potential security vulnerability

- **Embedded security:** Security for embedded systems.
  - usually strong limitation of **resources** and **complexity**
  - attacker often has **physical access** to the system

VEHICULAR IT SYSTEMS

Why use Vehicular IT Systems?

- **Cost reduction** (due to code reuse, easy copying, large-scale production of identical hardware)
- Less consumption of resources (i.e. fuel) due to **lower weight**
- Allows more sophisticated **functionality**:
  - can make driving **safer** and more convenient
  - allows **new business models** (e.g. pay-per-use content, after-sale applications)

VEHICULAR IT SYSTEMS

Why is Automotive IT Security getting increasingly important?

- An increasing amount of functionality is controlled by software
- Vehicular electronics are **more and more connected** (both internally and externally)
- **Standardization** of Hardware and Software
- New **legislations** and **business models**
- Upcoming **technology** (e.g. wireless **communication** to the outside world, electronic license plate) requires more security

PARTICULARITIES OF AUTOMOTIVE SECURITY

Pros

- **Updates** (e.g. security fixes) are possible (but not feasible for critical measures)
- Periodic inspections (attacks could be detected, but cannot be enforced and periods between inspections are long)
- **Vehicle is moving** (hard target for an external attacker)
- Rudimentary physical protection against external attacks (but no tamper-resistance)
- Sufficient **energy and space** compared to other embedded system
- Many different systems (i.e. harder to attack)
- Ongoing standardization between vendors

Cons

- Need **hard real-time** but limited resources
- Physically **challanging environment** (e.g. temperatures between -40°C and 120°C)
- **Long product life-cycle** and lifespan
- Limited external communication resources
- Updates will not affect all vehicles (yet)
- Limited (willingness for) **user interaction**
- Diverse areas of (distributed) functionality
- **Unfamiliar architecture** (without security)
- Subsystems developed independently
- Multitude of involved parties
- Large costs, little (promotional) benefit
- Liability and **legislation issues**

PART II: USE CASES

Applications of vehicular electronics and automotive security

THEFT PROTECTION

Classic security problem: Prevent unauthorized entities from using the car (authentication)

Traditional Solution

Mechanical Lock

Today

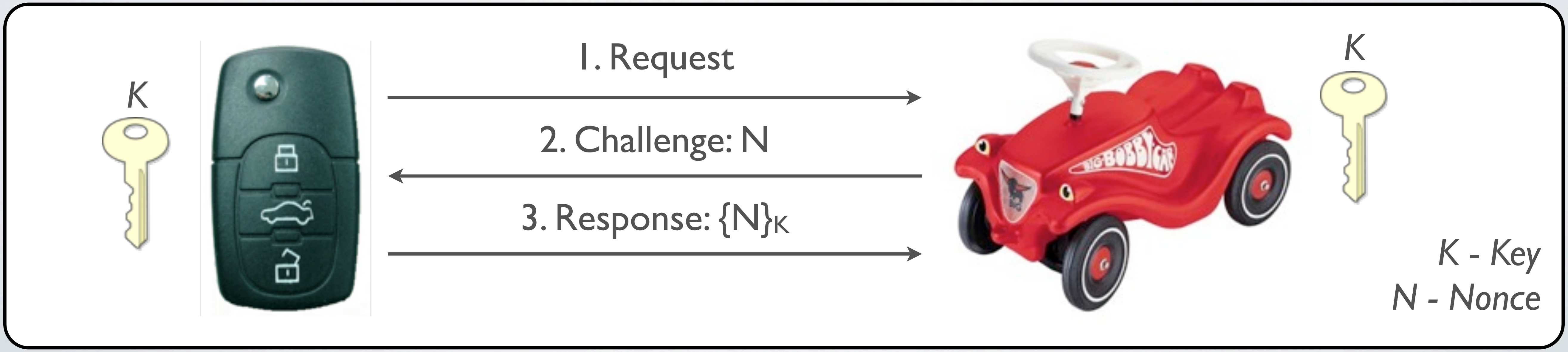
Electronic key, immobilizer

THEFT PROTECTION

Today: Electronic key, immobilizer

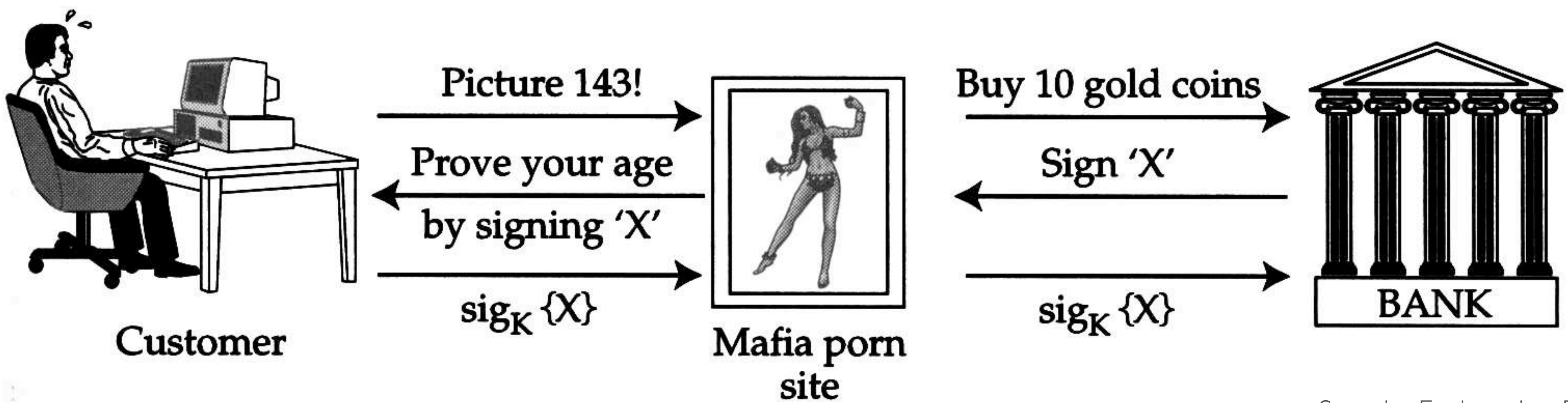
- Trivial solutions: Broadcast an ID that will unlock the car associated with it ➔ vulnerable against **replay attacks**

- More sophisticated: use **challenge-response protocols**



THEFT PROTECTION

- **Vendor-dependent**, **proprietary** solutions
- Security **distributed** over different devices and parts
- Main Threats: **Hardware attacks** (breaking the vehicle), **Replay attacks** (recording communication and replaying it), **Jamming attack** (denial of service), **Man-in-the-middle**

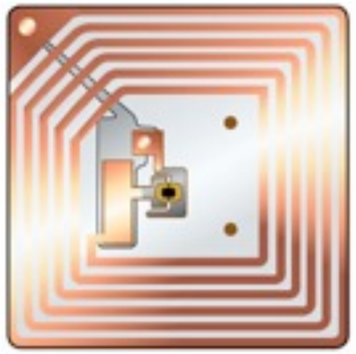


Security Engineering, First Edition, p. 25

COUNTERFEIT PROTECTION

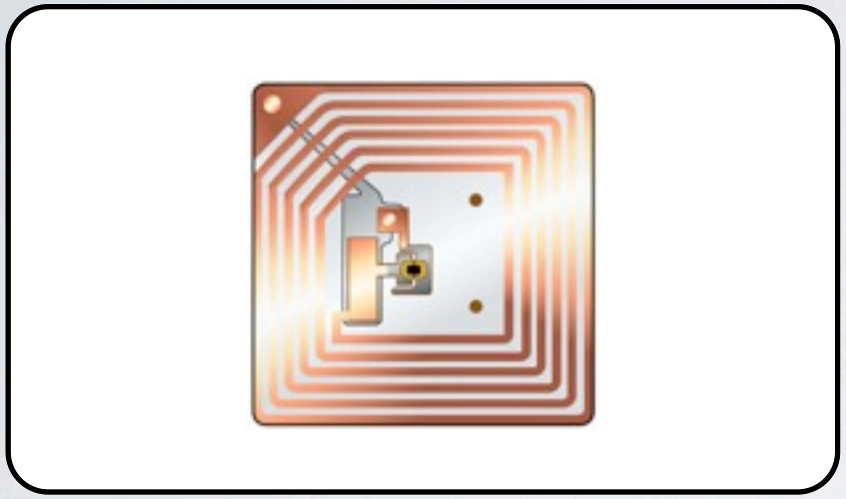
Prevent third parties from counterfeiting and selling parts
(causes huge losses of revenue and is potentially dangerous)
- related to protection of intellectual property

Traditional Solutions
holographic stickers, IDs, mechanical protection, seals



Future Solutions
Electronic component identification and binding

COUNTERFEIT PROTECTION



Future Solutions (Example)

- Electronic component **identification**
- **Binding** them to a particular vehicle

- Components are **tagged** (e.g. RFID chip)
- Each vehicle has a **secret key** (vehicle key)
- At installation, vehicle checks the component's tag (i.e. **certificate**) and transfers the vehicle key to the component
- Now the vehicle can **check** that all parts know the key

PROTECTION AGAINST TUNING

Detect and prevent unauthorized modification of software and components.

- Protect software by **cryptographic measures** (e.g. use **digital signatures**) - allows **detection** of modifications
- Threats:
  - Usage of **diagnosis tools** in an unauthorized way
  - Break the **cryptography**
  - Manipulate **hardware**

MILEAGE COUNTER

Another classical application: Measures the distance a car has traveled so far while being tamper-resistant

- Has to fulfill **legal requirements**
- Attacker would usually be **owner** or a garage
- Traditional solution: **Mechanical**, tamper-resistant counter
- Today: **Electronic** counter, cryptographic protection
- Threats: physical attacks (motion sensor, storage location, etc.), manipulating display, replacing counter

MILEAGE COUNTER

Approaches to protect against these attacks:

- **Spread storage** of the mileage count over multiple units
- Keep the functionality of the counter secret (**Security through Obscurity**) - **not desirable, but prevalent**
- Use some **physical protection** (tamper-resistance)
- **Bind** the counter to a particular vehicle (e.g. mechanically or cryptographically)
- Use **cryptographic measures** (e.g. monotonic counter using hash chains) to prevent mileage count from being changed

LICENSE PLATE

Allow identification of vehicles

- Traditional License Plates have **disadvantages**: cannot be read automatically, can easily be replaced or faked
- Alternative: **Electronic License Plate**
  - would allow **automatic identification**
  - new **applications** (e.g. automatic tolling, rental car return)
- Threats: privacy issues, counterfeiting, removal or replacement
- Hard to provide **anonymity** against unauthorized entities

EVENT DATA RECORDER

Similar to Digital Tachograph (and Electronic Logbook) but stores different events (e.g. lighting and safety belt status)

- Always stores the events of the **last couple of seconds**, e.g. belt status, speed, direction
- Can be used by insurance companies in **case of an accident** (or the vendor to enhance safety and find mistakes)
- Attacker is usually the **owner** or driver
- **Problem**: no incentive for drivers to use them

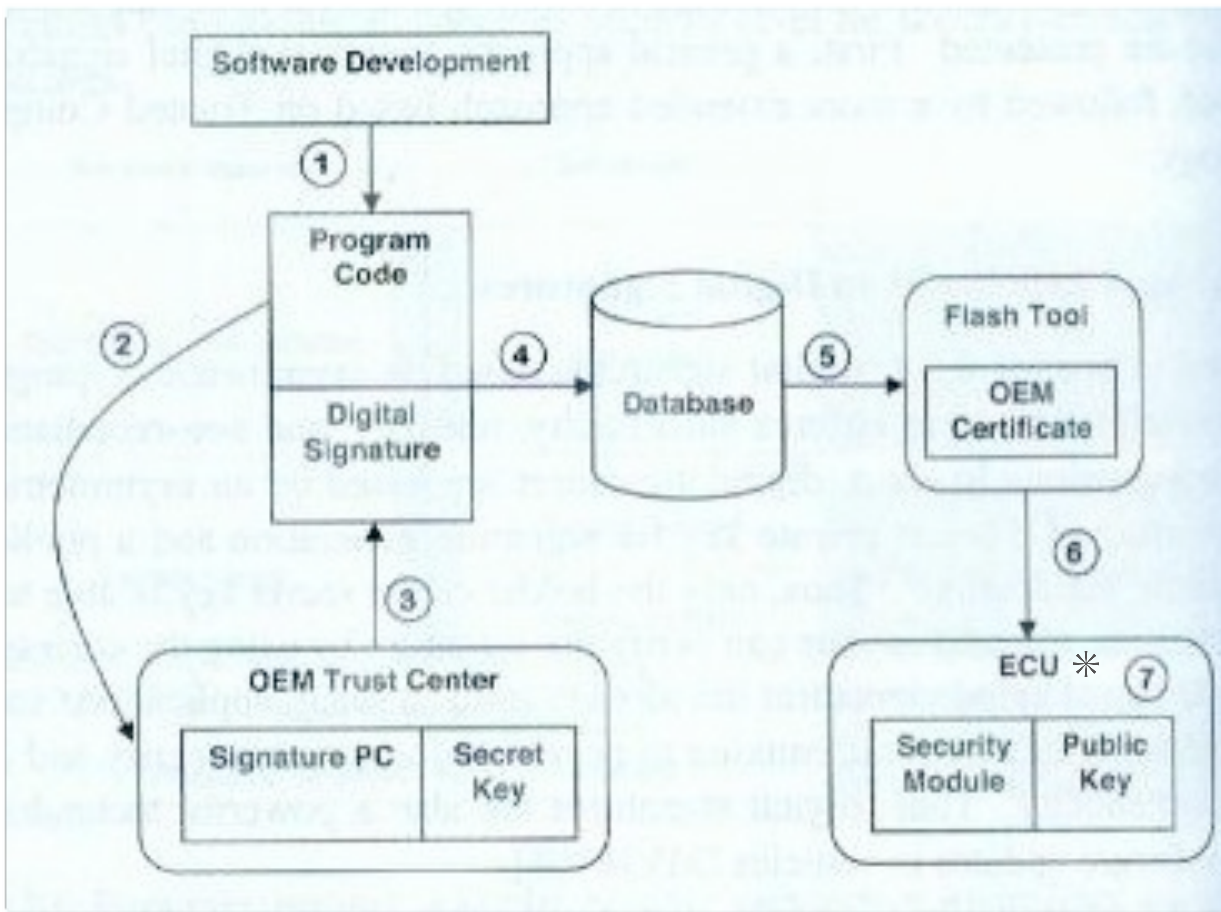
SOFTWARE UPDATES / FEATURE ACTIVATION

Replace software components after deploy of the vehicle

- Allows e.g. **security fixes** and **after-sale-applications** (i.e. build full set of features into every car but only activate those paid for), gives raise to **new business models**
- Acceptance of feature activation differs between **markets**
- **Security is crucial**, as bogus software updates could remove other security measures
- Threats: software manipulation, software theft

SOFTWARE UPDATES / FEATURE ACTIVATION

- Requires a method to perform **secure flashing**



Security for Vehicular IT Systems

*ECU = Electronic Control Unit

1. Developing software
2. Signing software in a trusted (protected) environment
3. Appending signature to the software / update
4. Storing both in a database
5. Transfering data to flash tool
6. Verifying signature and writing software to unit (7)

FUTURE APPLICATIONS

location-based services

electronic traffic signs

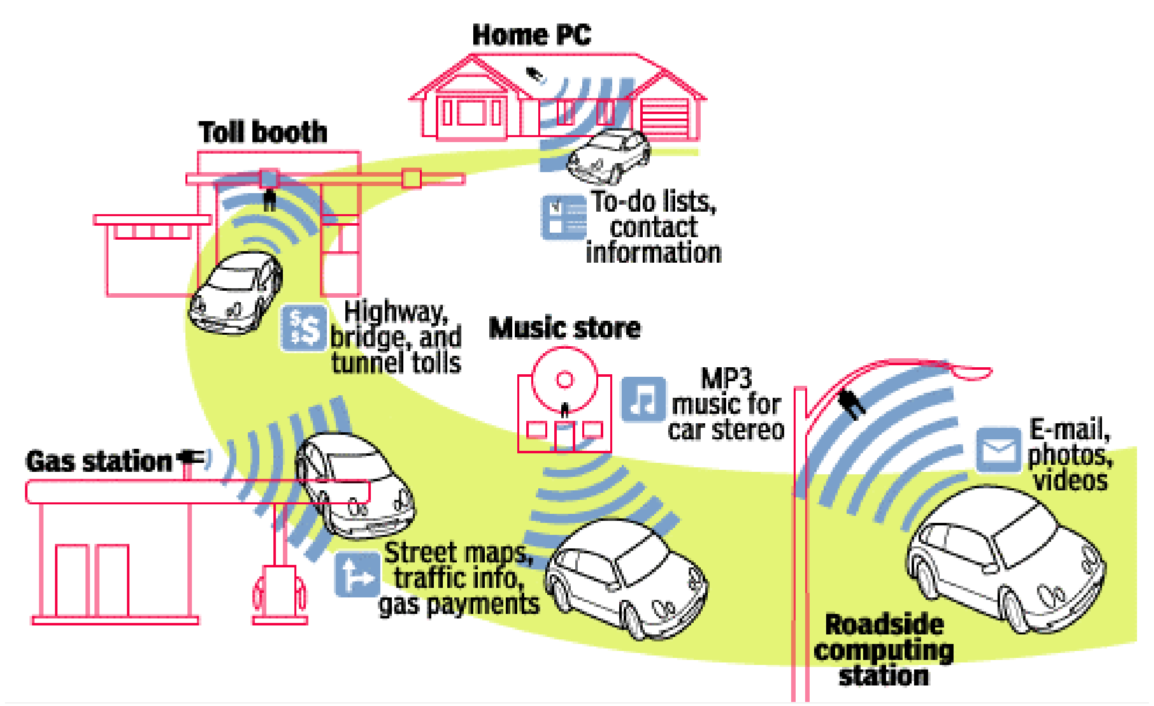
infotainment

on-demand content (maps, music,...)

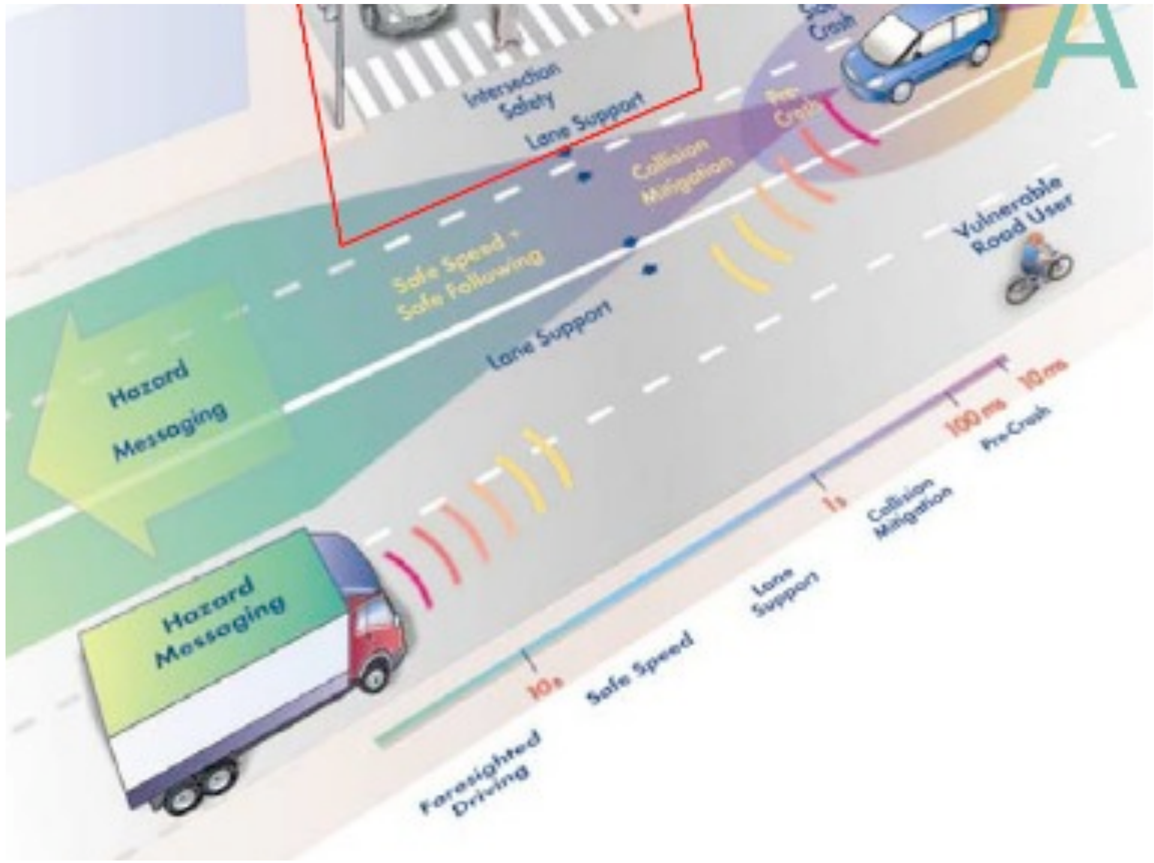
adaptive cruise control

drive by wire, automatic lane changing

FUTURE APPLICATIONS



V2V and V2I Communication, Dr. Wieland Holfelder
http://aswsd.ucsd.edu/2004/pdfs/V2VandV2ICommunication-Slides-WHolfelder.pdf



Security Engineering for Vehicular IT Systems, p. 69

V2I communication

e.g. automatic toll stations, gas stations could choose the fuel automatically

V2V communication

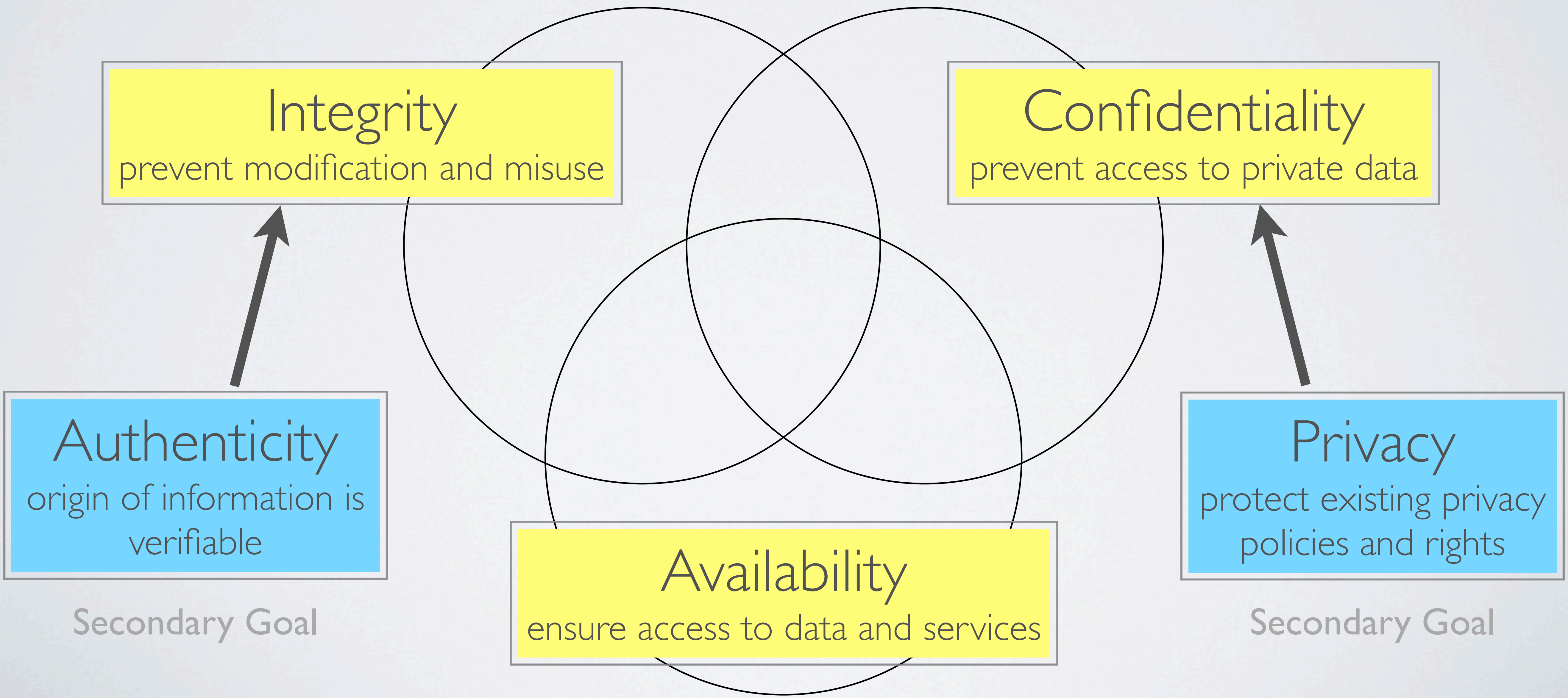
e.g. automatic hazard warnings, negotiate right of way automatically

PART III: SECURITY ENGINEERING

Approaches to implement security mechanisms and peculiarities of automotive security

SECURITY OBJECTIVES

Objectives differ between different data and services, but usually one or more of the following are required:



SECURITY OBJECTIVES

When designing a secure system...

1: Determine all potentially security-critical data that is involved and all entities interacting with the system

2a: Threat Analysis

2b: Risk Assessment

3: Identify the security objectives for each entity acting on each of the identified data (e.g. integrity, confidentiality)

Merge all objectives

Overall objectives for all pieces of data

CLASSIFYING ATTACKERS

- Attackers can be classified according to their **goals** (e.g. steal vehicle or intellectual property, manipulate records, circumvent restrictions), **access**, **financial resources** and **knowledge**
- Different approaches to evaluate them:
  - **Common criteria**: Defines ways to measure **parameters** and use them to calculate an **attack potential**

```
Expertise x Resources x Motivation → Attack potential
```

  - **Simpler approach**: Divide attackers into four **classes** **External** attackers (E) and **Internal** attackers (I_1-I_3)

CLASSIFYING ATTACKERS

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

	Attacker I_1 Internal Class I	**Attacker I_2** Internal Class II	**Attacker I_3** Internal Class III	**Attacker E_0** External Class 0
Exemplary attackers	Driver, owner	Motor mechanics, backyard garage	Organized crime, rival, academia	Thief, V2I or V2V mischief
Physical access	Limited to resp. skills	Extensive, but not unlimited	Virtually unlimited	None or only very limited
Technical resources	Generally low	Medium to high	Very high	Varies, usually low to medium
Knowledge resources	Generally low	Medium to high	Very high	Varies, but can be high
Financial resources	Low	Medium	Very high	Generally low
Reliable protection	Mostly feasible	Varies, but still feasible	Only by econ. security	Mostly feasible

Common Criteria 3.1

CLASSIFYING ATTACKS

- **Logical attacks** (internal/external):
  - Cryptographic attack (e.g. Brute Force)
  - Software attack (e.g. Buffer Overflow)
  - Communication attack (e.g. wiretapping)
- **Physical attacks** (always internal):
  - Side-channel attack
  - Denial of service (often trivial)
  - Modification, penetration, fault attacks

SECURITY (FUNCTIONAL) REQUIREMENTS

- Security requirements specify the actual measures to fulfill the determined security objectives
- Depend on making assumptions about the environment, taking care of potential threats and existing policies

It is **not** necessary to choose a method that is "**impossible**" to break. It solely has to be **hard enough** to make it **unfeasible** for an attacker. (**Economic Security**)

It is not only necessary to make sure that the **right methods** have been chosen. It is as well necessary to consider their **interactions** and make sure they are being **applied correctly**

SECURITY (FUNCTIONAL) REQUIREMENTS

Examples for security measures:

- **Component identification** (authenticity)
- **Secure initialization** (authenticity, integrity)
- **Secure audit** (authenticity, availability, integrity), e.g. for Electronic Data Recorders
- **Secure storage** (authenticity, confidentiality integrity)
- **Strong isolation** (of subsystems)
- **Security through Obscurity** (not desirable but prevalent)

Most of these measures are not used in the automotive domain yet.

IMPLEMENTATION: PHYSICAL PROTECTION

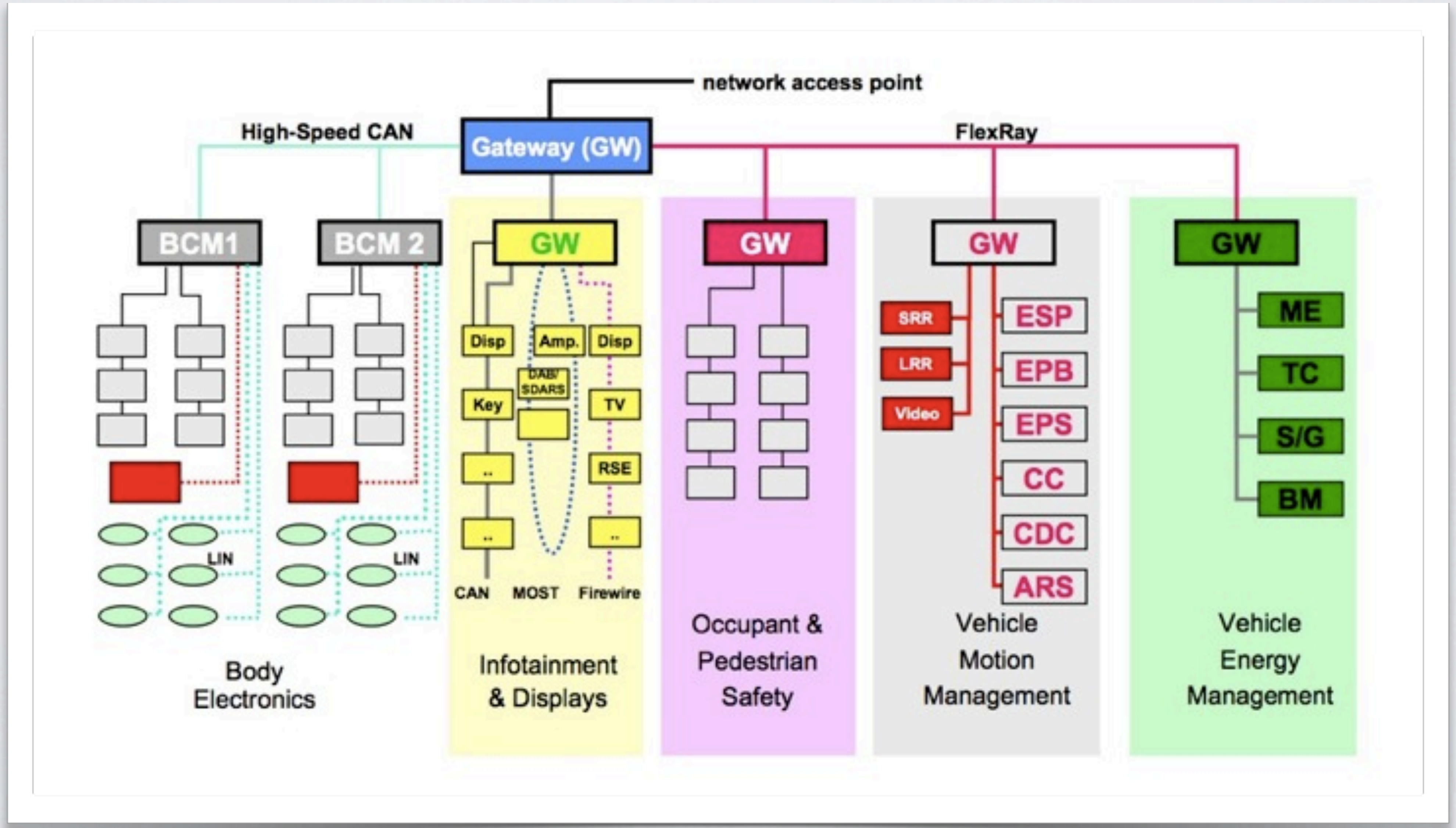
- One of the main security features **used today**
- Usually the **first layer of protection**, but only works in combination with other methods
- Different types:
    - **Tamper-evidence** (passive, e.g. seals, etc.)
    - **Tamper-resistance** (passive, e.g. special cases, security screws, very small chips, etc.)
    - **Tamper-response** (active, e.g. delete secrets, self-destruction, etc.)

IMPLEMENTATION: SECURITY MODULES

- **Not being used** in the automotive domain yet but one potential way of handling many different security problems
- Provides **basic security services** and handles all security-critical data (e.g. secret keys, etc.)
- Security modules s.t. use **Trusted Computing Technology**, i.e. systems incorporating methods to ensure **authenticity**, **integrity**, **confidentiality** of its content (i.e. software and data)
- System can use a **single** Security Module (central/semi-central) or functionality can be **distributed**

IMPLEMENTATION: INTERNAL NETWORKS

- Vehicular IT systems usually have a **multitude** of different **internal networks**, connected by gateways



The car of today and tomorrow, In-Vehicle LAN

IMPLEMENTATION: INTERNAL NETWORKS

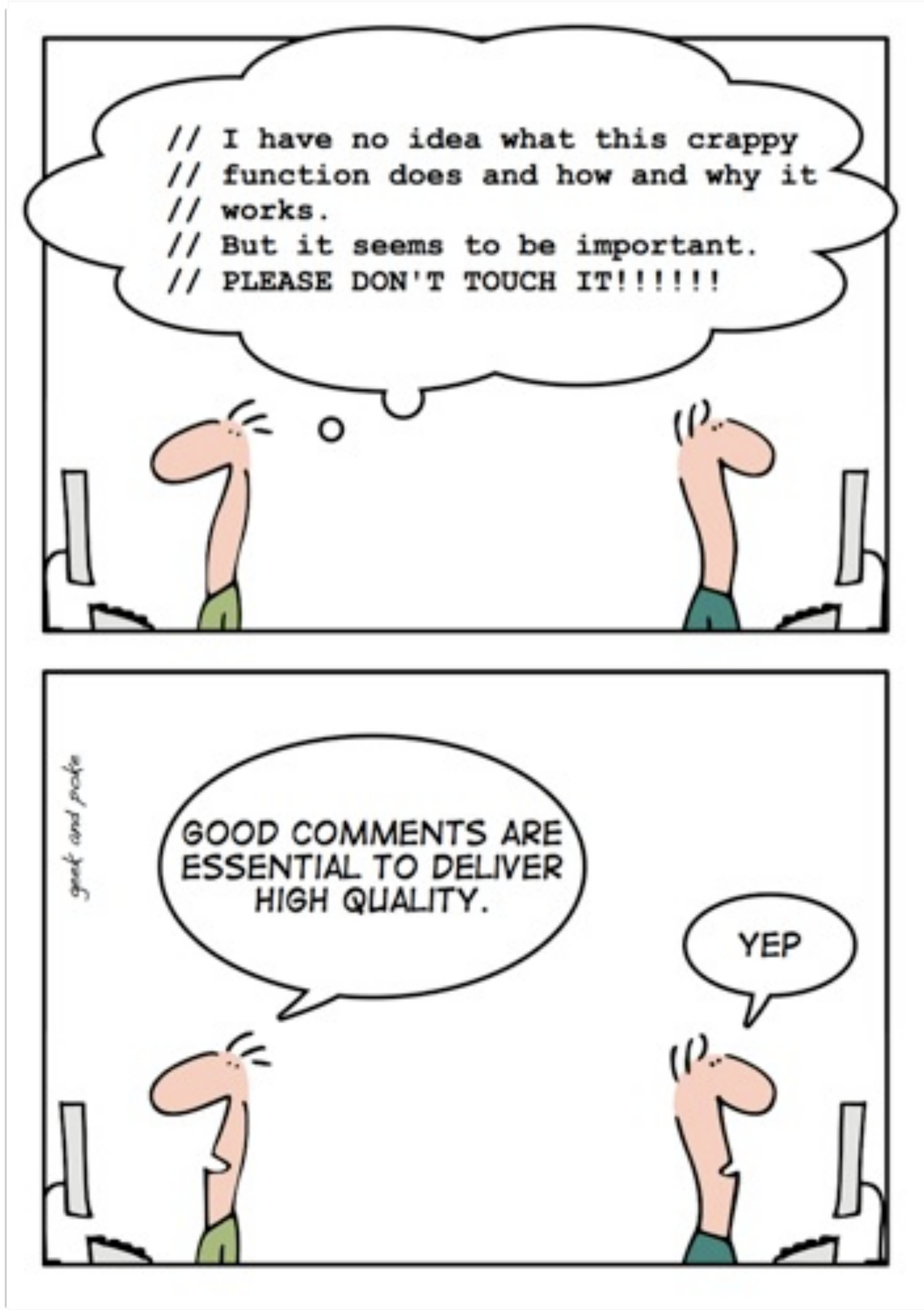
- **Security-critical**, but today mostly **unprotected**
- Could be protected by **appropriate methods**:
  - **Controller authentication**
  - **Intrusion detection**
  - **Bus encryption**
  - **Gateway firewalls** (e.g. based on MACs)

None of this happens in real-world applications today.

ORGANIZATIONAL SECURITY

- Protection against **Social Engineering** at least as important as technical security
- Leaked information can **damage company's reputation**, give away **trade secrets**, intruders could introduce **backdoors**
- Procedure to establish organizational security: Determine **critical assets**, **potential attacks** and **trustworthiness of environments** (e.g. service, maintenance, manufacturing environments are very insecure)
- Establish **security policies**

ORGANIZATIONAL SECURITY



- Establish **understanding** of **reason** for measures
- (Security) policies have to be **realistic** and enforceable
- **Prevent unchecked code** from getting into the software, **restrict** access to all test versions, divide into sub-projects
- Prevent personnel from changing to competitors
- Make theft of information **identifiable** (e.g. by well-placed misinformation)

SUMMARY

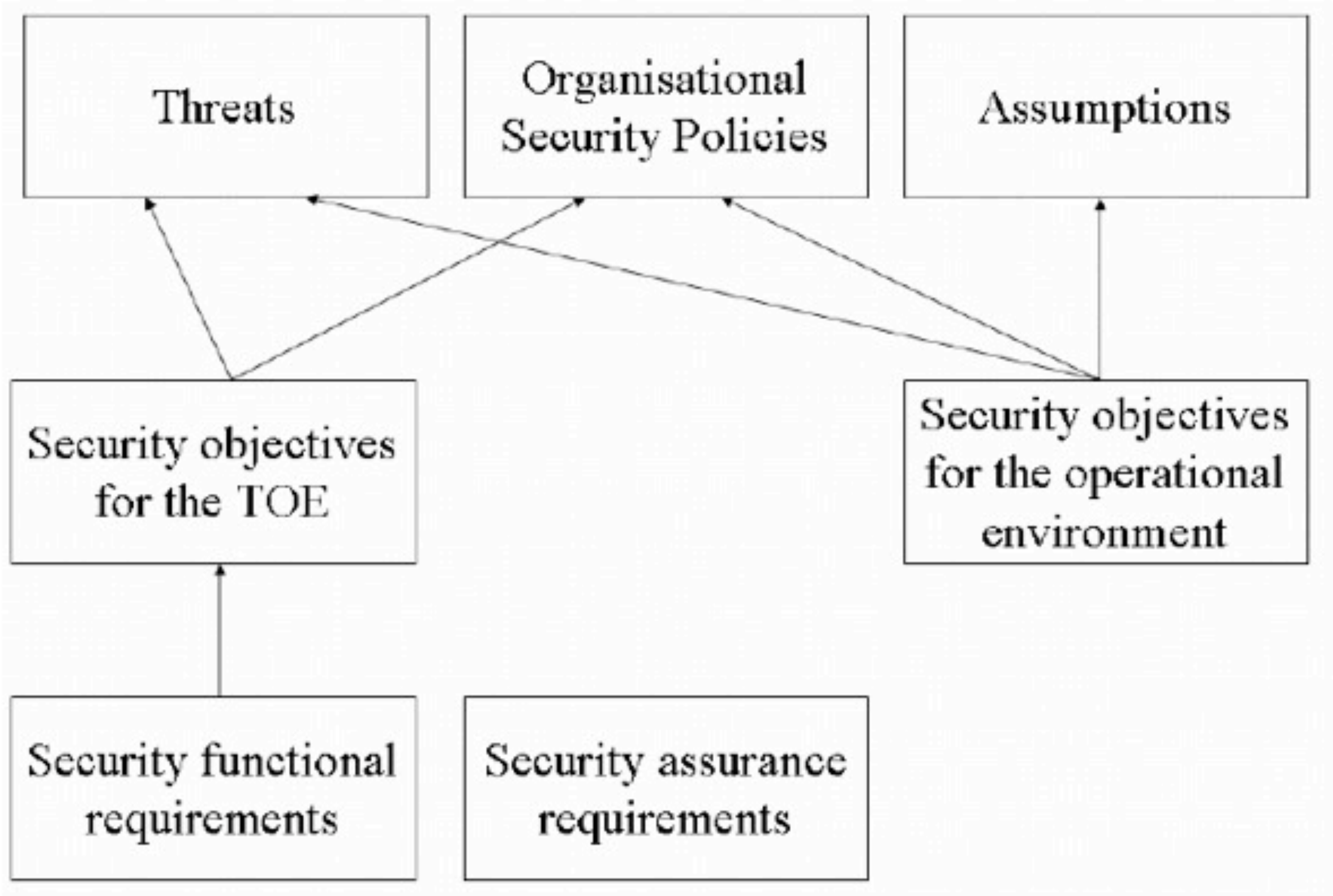


Figure 7 - Relations between the security problem definition, the security objectives and the security requirements

PART IV: PERSPECTIVES

The future of automotive security

THESES

- Vehicular IT systems will become more and more important and so will vehicular security
- Especially the broad introduction of V2I and V2V communication will lead to a significant increase of work (and progress) in this area
- There will be ongoing standardization in the field of Vehicular IT Security
- There will be much legislation related to it

PART IV: DISCUSSION

Questions and Free Discussion

THANK YOU!

- Sources:
  - **Security Engineering for Vehicular IT Systems**, Marko Wolf, Vieweg + Teubner 2009
  - **Security Engineering Second Edition**, Ross Anderson, Wiley, 2008
  - **Wikipedia**: Security Engineering
  - Common Criteria Version 3.1
  - The car of today and tomorrow, Vehicle In-LAN
    http://www.vehiclelan.com/eng/vehicles-today-and-tomorrow.html